Accademia delle competenze di cybersecurity

Cybersecurity Skills Academy

TOPIC ID:
DIGITAL-2023-SKILLS-05-CYBERACADEMY

Ente finanziatore:
Commissione europea
Programma Europa digitale (DIGITAL)

Obiettivi ed impatto attesi:
Obiettivo:
La sicurezza informatica è diventata una preoccupazione crescente per i cittadini, le imprese e le autorità pubbliche europee. Oltre ai cittadini qualificati, l'UE ha bisogno di un maggior numero di specialisti in cybersecurity per proteggere le imprese e i servizi pubblici in Europa e progettare le soluzioni di cybersecurity del futuro. Attualmente in Europa mancano circa 200.000 esperti di cybersecurity. Le recenti iniziative legislative, come la NIS2 e l'imminente Cyber Resilience Act, eserciteranno una pressione ancora maggiore sulle aziende e sulle autorità pubbliche affinché abbiano accesso agli specialisti di cybersecurity. Per affrontare queste sfide, la Commissione europea ha già messo in campo molte azioni, in stretta collaborazione con gli attori interessati. Tuttavia, le azioni e le risorse sono spesso percepite come disperse e inaccessibili. La Cybersecurity Skills Academy costituirebbe un ombrello europeo che integra diverse attività con l'obiettivo di aumentarne la visibilità, l'accessibilità e l'impatto. Queste attività si allineerebbero su obiettivi comuni, indicatori chiave di performance e una strategia di comunicazione congiunta per ottenere un maggiore impatto.
Ambito di applicazione:
La Cybersecurity Skills Academy; programmi di formazione per le PMI, le start-up e il settore pubblico Saranno disponibili finanziamenti per l'implementazione di nuove opportunità di formazione o per l'ampliamento di quelle già esistenti, con particolare attenzione alle esigenze delle PMI e della pubblica amministrazione nel campo della cybersecurity. Le formazioni dovranno tenere conto delle esigenze delle imprese e in particolare facilitare l'accesso ai talenti della cybersecurity per le PMI e le start-up di tutti i settori. Per garantire gli elevati livelli di cybersecurity necessari alla pubblica amministrazione digitale, l'Accademia dovrebbe provvedere all'aggiornamento, alla riqualificazione e alla comprensione interdisciplinare della cybersecurity per i dipendenti pubblici. Consorzi di organizzazioni attive nel settore della cybersecurity e università o enti di formazione dovrebbero ideare e realizzare le attività dell'Accademia. Le attività dovrebbero comprendere, tra l'altro, l'individuazione di corsi di formazione pertinenti, compresi i bootcamp su argomenti specifici di cybersecurity, vagliati congiuntamente con partner industriali che migliorerebbero l'occupabilità dei tirocinanti o aumenterebbero le capacità di cybersecurity dei dipendenti pubblici, azioni di comunicazione per promuovere i corsi, ecc. Il coinvolgimento dei centri nazionali di competenza in materia di cybersecurity potrebbe essere previsto per rispondere a esigenze specifiche a livello nazionale, dove esistono variazioni significative per quanto riguarda il livello di preparazione alla cybersecurity. Creazione e gestione dell'Accademia delle competenze

in materia di cibersicurezza
• Definizione di una serie di KPI chiari per misurare l'impatto delle diverse azioni considerate nell'ambito dell'Accademia.
• Riunire gli attori rilevanti di tutti gli Stati membri per monitorare il panorama delle competenze in materia di cybersecurity, seguirne l'evoluzione e intervenire per aiutare gli Stati membri a sviluppare programmi di formazione specializzati, rivolgendosi in particolare alle start-up e alle PMI che si occupano di cybersecurity e alle amministrazioni pubbliche per colmare il deficit di competenze in materia di cybersecurity.
• Esplorare, definire e istituire uno schema d'impatto che promuova la standardizzazione delle procedure per il riconoscimento delle competenze di cybersecurity e la certificazione professionale nel mercato europeo.
• Promuovere lo sviluppo e l'utilizzo di programmi di studio aggiornati in materia di cybersicurezza.
• Realizzare la comunicazione intorno a questa iniziativa, per coinvolgere le parti interessate e facilitare le interazioni tra queste ultime.
• Sfruttare la piattaforma Digital Skills & Jobs per supportare l'Accademia e integrare le best practice esistenti che alimenteranno l'Accademia.
Risultati e risultati attesi:
Corsi di formazione per affrontare le competenze più richieste, come la cyber-forensics, le gamme informatiche, l'analisi delle minacce informatiche e l'IA per la cybersecurity.
• Corsi di formazione on the job e opportunità di tirocinio per start-up e PMI e per le pubbliche amministrazioni in aziende innovative nel campo della cybersecurity e dei centri di competenza sulla cybersecurity
• Formazione online, facile da usare e accessibile a tutti, in tutte le lingue.
• Schema per l'istituzione di un riconoscimento delle competenze di cybersecurity e di una certificazione professionale nel mercato europeo 74
• Quadro dei KPI e suo monitoraggio, anche attraverso indicatori misurabili, per tutta la durata dell'azione

Criteri di eleggibilità:
Per essere ammissibili, i richiedenti (beneficiari ed enti affiliati) devono:
- essere persone giuridiche (enti pubblici o privati)
- essere stabilito in uno dei paesi ammissibili, ossia:
- Stati membri dell'UE (compresi i paesi e territori d'oltremare (PTOM))
- Paesi non appartenenti all'UE:
- Paesi SEE elencati e Paesi associati al Programma Europa Digitale (Paesi associati) o Paesi che hanno in corso negoziati per un accordo di associazione e in cui l'accordo entra in vigore prima della firma della sovvenzione I beneficiari e le entità affiliate devono registrarsi nel Registro dei Partecipanti - prima di presentare la proposta - e dovranno essere convalidati dal Servizio Centrale di Convalida (REA Validation). Per la convalida, sarà richiesto loro di caricare documenti che dimostrino lo status giuridico e l'origine. Altre entità possono partecipare in altri ruoli del consorzio, come partner associati, subappaltatori, terze parti che forniscono contributi in natura, ecc.
I consorzi che richiedono un finanziamento nell'ambito di questa tematica possono essere composti dai seguenti tipi di soggetti: istituti di istruzione superiore, istituti di istruzione e formazione professionale, servizi della pubblica amministrazione, organizzazioni di ricerca, imprese e centri nazionali di competenza

in materia di cibersicurezza.
- Per questo tema, le domande multi-beneficiario sono obbligatorie e si applicano condizioni specifiche per la composizione dei consorzi.

Contributo finanziario:
Il budget disponibile per l'invito è di 5 800 000 EUR.
Budget del progetto Per la priorità 1 (questioni civili) e la priorità 4 (ECRIS): la sovvenzione UE richiesta non può essere inferiore a 75 000 euro.
Non c'è un limite massimo. Per la priorità 2 (questioni penali) e la priorità 3 (EJN civile e penale):
I budget dei progetti devono essere compresi tra 75 000 e 350 000 euro per progetto.
La sovvenzione concessa può essere inferiore all'importo richiesto.
I parametri della sovvenzione (importo massimo della sovvenzione, tasso di finanziamento, costi totali ammissibili, ecc.) saranno stabiliti nella Convenzione di sovvenzione (Scheda tecnica, punto 3 e art. 5).
Bilancio del progetto (importo massimo della sovvenzione)
La sovvenzione concessa può essere inferiore all'importo richiesto. La sovvenzione sarà una sovvenzione forfettaria. Ciò significa che rimborserà un importo fisso, basato su una somma forfettaria o su un finanziamento non legato ai costi. L'importo sarà fissato dall'autorità concedente sulla base del budget stimato del progetto e di un tasso di finanziamento del 90%.

Scadenza:
21 marzo 2024 17:00:00 ora di Bruxelles

Ulteriori informazioni:
call-fiche_digital-2023-skills-05_en.pdf (europa.eu)